附录 K
（规范性附录）
银联卡闪付联机小额免密产品境内收单方案

K.1 基于SM4 的硬件序列号加密算法

a)由[硬件序列号+加密随机因子]构成MAC ELEMEMENT BLOCK （MAB）。

b) SM4算法的MAB，按每16个字节做异或（不管信息中的字符格式），如果最后不满16个字节，则添加“0X00”。

示例：

MAB = M1 M2 M3M4

其中：

M1 = MS01 MS02 MS03 MS04 MS05 MS06 MS07 MS08 MS09 MS10 MS11 MS12 MS13 MS14 MS15 MS16

M2 = MS21 MS22 MS23 MS24 MS25 MS26 MS27 MS28 MS29 MS30 MS31 MS32 MS33 MS34 MS35 MS36

M3= MS41 MS42 MS43 MS44 MS45 MS46 MS47 MS48 MS49 MS50 MS51 MS52 MS53 MS54 MS55 MS56

M4= MS61 MS62 MS63 MS64 MS65 MS66 MS67 MS68 MS69 MS70 MS71 MS72 MS73 MS74 MS75 MS76

按如下规则进行异或运算：

MS01 MS02 MS03 MS04 MS05 MS06 MS07 MS08 MS09 MS10 MS11 MS12 MS13 MS14 MS15 MS16

XOR）

MS21 MS22 MS23 MS24 MS25 MS26 MS27 MS28 MS29 MS30 MS30 MS32 MS33 MS34 MS35 MS36

RESULT BLOCK1 = TM01 TM02 TM03 TM04 TM05 TM06 TM07 TM08 TM09 TM10 TM11 TM12 TM13 TM14 TM15 TM16

进行下一次异或

TM01 TM02 TM03 TM04 TM05 TM06 TM07 TM08 TM09 TM10 TM11 TM12 TM13 TM14 TM15 TM16

XOR）

MS41 MS42 MS43 MS44 MS45 MS46 MS47 MS48 MS49 MS50 MS51 MS52 MS53 MS54 MS55 MS56

RESULT BLOCK2 = TM21 TM22 TM23 TM24 TM25 TM26 TM27 TM28 TM29 TM30 TM31 TM32 TM33 TM34 TM35 TM36

再进行一次异或运算

TM21 TM22 TM23 TM24 TM25 TM26 TM27 TM28 TM29 TM30 TM31 TM32 TM33 TM34 TM35 TM36

XOR）

MS61 MS62 MS63 MS64 MS65 MS66 MS67 MS68 MS69 MS70 MS71 MS72 MS73 MS74 MS75 MS76

RESULT BLOCK = TM41 TM42 TM43 TM44 TM45 TM46 TM47 TM48 TM49 TM50 TM51 TM52 TM53 TM54 TM55 TM56

c) 将异或运算后的最后16个字节（RESULT BLOCK）转换成32 个HEXDECIMAL：

RESULT BLOCK = TM41 TM42 TM43 TM44 TM45 TM46 TM47 TM48 TM49 TM50 TM51 TM52 TM53 TM54 TM55 TM56

= TM011 TM012 TM021 TM022 TM031 TM032 TM041 TM041 TM051 TM052 TM061 TM062 TM071 TM072 TM081 TM082 || TM091 TM092 TM101 TM102 TM111 TM112 TM121 TM122 TM131 TM132 TM141 TM142 TM151 TM152 TM161 TM162

d) 取前16 个字节用SM4加密：

ENC BLOCK1 = SM4K （ TM011 TM012 TM021 TM022 TM031 TM032 TM041 TM041 TM051 TM052 TM061 TM062 TM071 TM072 TM081 TM082）

= EN 011 EN 012 EN 021 EN 022 EN 031 EN 032 EN 041 EN 041 EN 051 EN 052 EN 061 EN 062 EN 071 EN 072 EN 081 EN 082

e) 将加密后的结果与后16 个字节异或：

EN 011 EN 012 EN 021 EN 022 EN 031 EN 032 EN 041 EN 041 EN 051 EN 052 EN 061 EN 062 EN 071 EN 072 EN 081 EN 082

XOR）TM091 TM092 TM101 TM102 TM111 TM112 TM121 TM122 TM131 TM132 TM141 TM142 TM151 TM152 TM161 TM162

TEMP BLOCK=TE01 TE02 TE03 TE04 TE05 TE06 TE07 TE08 TE09 TE10 TE11 TE12 TE13 TE14 TE15 TE16

f) 用异或的结果TEMP BLOCK 再进行一次SM4密钥算法运算。

ENC BLOCK2 = SM4K（TE01 TE02 TE03 TE04 TE05 TE06 TE07 TE08 TE09 TE10 TE11 TE12 TE13 TE14 TE15 TE16）

= EN21 EN22 EN23 EN24 EN25 EN26 EN27 EN28 EN29 EN30 EN31 EN32 EN33 EN34 EN35 EN36

g) 将运算后的结果（ENC BLOCK2）转换成32 个HEXDECIMAL：

ENC BLOCK2 = EN21 EN22 EN23 EN24 EN25 EN26 EN27 EN28 EN29 EN30 EN31 EN32 EN33 EN34 EN35 EN36

= EN211 EN212 EN221 EN222 EN231 EN232 EN241 EN242 EN251 EN252 EN261 EN262 EN271 EN272 EN281 EN282||

EN291 EN292 EN301 EN302 EN311 EN312 EN321 EN322 EN331 EN332 EN341 EN342 EN351 EN352 EN361EN362

ENC RESULT

= %H84, %H56, %HB1, %HCD, %H5A, %H3F, %H84, %H84%H84, %H56, %HB1, %HCD, %H5A, %H3F, %H84, %H84

转换成32 个HEXDECIMAL：

“8456B1CD5A3F84848456B1CD5A3F8484”

h) 取前8个字节作为硬件序列号加密数据。

取“8456B1CD”为硬件序列号加密数据。